Secure Silicon: Towards Virtual Prototyping

Laurent Sauvage[a,b], Sofiane Takarabt[a], Youssef Souissi[a]

[a] *LTCI, CNRS, Télécom ParisTech, Université Paris-Saclay*
75013 Paris, France
[b] *Secure-IC*
15 rue Claude Chappe, 35510 Cesson-Sévigné, France

Abstract

Evaluating security vulnerabilities of software implementations at design step is of primary importance for applications developers, while it has received litte attention from scientific communauty. In this paper, we describe virtual prototyping of an implementation of Elliptic curve cryptography (ECC), aiming to make it secure against first-order horizontal and vertical side-channel attacks (SCAs). Reproducing information leakage as close to reality as possible requires bit- and clock-cycle accuracy, we got with Mentor Graphics Modelsim tool, simulating the execution of the ECC software implementations on PULPino, an open-source 32-bit microcontroller based on the recently released RISC-V instruction set architecture. For each clock cycle, we compute the number of bit toggles into microcontroller's registers, an image of the power consumption, and watch the program counter to identify the assembly instruction executed, then the corresponding C function. We first start with a naive double-and-add implementation relying on cryptographic primitives of the mbed TLS library, formerly PolarSSL before acquisition by ARM. The virtual analysis pinpoints differences in the way the double function on one side and the add function on the other side manage variables and internal operations, which can be used for horizontal SCAs. We propose some modifications of the C code, hence independent of the considered microcontroller, with an overhead extremely small compared to that of the double-and-add-always countermeasure. Then, we reiterate analyses, still for the mbed TLS library, but using the regular Montgomery ladder version, most used in practice as more efficient.

Keywords: Side-channel attack, simulation, elliptic curve cryptography, software implementation, mbed TLS, 32-bit RISC-V core